Dell PowerStore

Configuring NFS

4.1

February 2025
Rev. A07

DELL Technologies

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2020 - 2025 Dell Inc. or its subsidiaries. All rights reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

Preface

As part of an improvement effort, revisions of the software and hardware are periodically released. Some functions that are described in this document are not supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information about product features. Contact your service provider if a product does not function properly or does not function as described in this document.

NOTE: PowerStore X model customers: For the latest how-to technical manuals and guides for your model, download the *PowerStore 3.2.x Documentation Set* from the PowerStore Documentation page at dell.com/powerstoredocs.

Where to get help

Support, product, and licensing information can be obtained as follows:

- **Product information**—For product and feature documentation or release notes, go to the PowerStore Documentation page at dell.com/powerstoredocs.
- **Troubleshooting**—For information about products, software updates, licensing, and service go to Dell Support and locate the appropriate product support page.
- **Technical support**—For technical support and service requests, go to Dell Support and locate the **Service Requests** page. To open a service request, you must have a valid support agreement. Contact your Sales Representative for details about obtaining a valid support agreement or to answer any questions about your account.

1

Overview

This chapter contains the following information:

Topics:

NFS support

PowerStore T model and PowerStore Q model support NFSv3 and NFSv4. These models also support secure NFS with Kerberos, for strong authentication. While PowerStore T model and PowerStore Q model support most of the NFSv4 and v4.1 functionality described in the relevant RFCs, directory delegation and pNFS are not supported. In PowerStoreOS 3.0 and later, basic support for NFSv4.2 in compatibility mode is also available.

NFS support is enabled on a NAS server during or after creation, enabling you to create NFS-enabled file systems on that NAS server.

About secure NFS

You can configure secure NFS when you create or modify a NAS server that supports UNIX shares. Secure NFS provides Kerberos-based user authentication, which can provide network data integrity and network data privacy.

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services.

Security options

Secure NFS supports the following security options:

- krb5: Kerberos authentication
- krb5i: Kerberos authentication and data integrity by adding a signature to each NFS packet transmitted over the network
- krb5p: Kerberos authentication, data integrity, and data privacy by encrypting the data before sending it over the network

  Data encryption requires more resources for system processing and can lead to slower performance.

In a secure NFS environment, user access to NFS file systems is granted based on Kerberos principal names. However, access control to shares within a file system is based on the UNIX UID and GID, or on ACLs.

NOTE: Secure NFS supports NFS credentials with more than 16 groups, which is equivalent to the extended UNIX credentials option.

Configuring secure NFS

If you are implementing Secure NFS, configure the following:

- At least one NTP server must be configured on the PowerStore appliance to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure.
- A UNIX Directory Service (UDS)
- One or more DNS servers

- Either an AD or custom realm must be added for Kerberos authentication
- A keytab file must be uploaded to your NAS server when using a custom realm in a Kerberos configuration

Planning considerations

Review the following information before configuring NFS exports:

File storage support is only available with PowerStore T model and PowerStore Q model appliances.

NAS server networks

Creating network VLANs and IP addresses is optional for NAS servers. If you plan to create a VLAN for NAS servers, the VLAN cannot be shared with the PowerStore T model and the PowerStore Q model management, or storage networks. Also, be sure to work with your network administrator to reserve the network resources and configure the network on the switch. See the *PowerStore T and Q Networking Guide for Storage Services* for details.

Scalability

In PowerStoreOS 3.5 and later, there is a shared limit for file systems volumes and vVols. The total number of objects is determined according to the highest limit of the three object types.

To view the limit for file systems per platform, see *Dell Technologies PowerStore Simple Support Matrix* on the PowerStore Documentation page.

Deployment requirements

NAS services are only available on PowerStore T model and PowerStore Q model appliances.

You must have chosen **Unified** during initial configuration of your PowerStore T model and PowerStore Q model appliances. If you chose **Block Optimized** while running the Initial Configuration Wizard, NAS services were not installed. To install NAS services, a technical support representative must reinitialize your system. Reinitializing the system:

- Sets the appliance back to the factory state.
- Removes all configuration that was done on the system through the **Initial Configuration Wizard**.
- Removes any configuration that is performed in PowerStore after initial configuration.

More considerations

Both nodes on the appliance must be up and running to create a NAS server. If one of the nodes is down on the appliance, NAS server creation will fail.

Create the network interface for NAS traffic

You can configure a NAS network using Link Aggregation Control Protocol (LACP) bonds or by creating a Fail-Safe Network for NAS traffic.

Create LACP bonds for NAS traffic

If your switches are configured with MC-LAG, you can use network bonding by creating a Link Aggregate Group (LAG) for NAS traffic.

When the Top-of-Rack (ToR) switches are configured with an MC-LAG interconnect, it is recommended to configure the NAS interface over LACP bonds using Link Aggregation Groups (LAG). LACP bonding is a process in which two or more network interfaces are combined to a single interface. Using LACP bonding provides performance improvements and redundancy by increasing the network throughput and bandwidth. If one of the combined interfaces is down, the other interfaces are used to maintain a stable connection.

1. Select **Hardware** > **[Appliance]** > **Ports**.
2. From the ports list, select two to four ports of the same speed on the node on which you want to aggregate for Link Aggregate Control Protocol (LACP) Bond to service NAS traffic.

   NOTE: The configuration is symmetrical across the peer node.

3. Select **Link Aggregation** > **Aggregate Links**.
4. Optionally, provide a description for the bond.
5. Select **Aggregate**.
6. Scroll through the ports list and locate the generated bond name.

   NOTE: You must select the bond name when you create the NAS server.

Create a Fail-Safe Network

A Fail-Safe Network (FSN) should be created when the Top-of-Rack (ToR) switches have not been configured with an MC-Lag interconnect. An FSN extends link failover into the network by providing switch level redundancy. An FSN can be configured on a port, a link aggregation, or any combination of the two.

1. Select **Hardware** > **[Appliance]** > **Ports**.
2. If you plan to use aggregated links for the FSN, first create the Link Aggregation Groups. For details, see Create LACP bonds for NAS traffic.
3. From the list, select two ports or two link aggregations, or a combination of a port and a link aggregation group that you want to use for the FSN on node A and select **FSN** > **Create FSN**.
4. In the **Create FSN** panel, select which ports or link aggregation to use as the primary (active) network.

   NOTE: The primary port cannot be modified once it is used to create a NAS server.

5. Optionally, add a description of the Fail-Safe Network.
6. Click **Create**.

   PowerStore Manager automatically creates a name for the Fail-Safe Network using the format: "BaseEnclosure-<Node>-fsn<nextLACPbondcreated>"

   - BaseEnclosure is constant.
   - Node is the node that is displayed in the **Node-Module-Name** list.
   - nextLACPbondcreated is a numeral value that is determined by the order in which the bond was created in PowerStore Manager, starting with zero for the first created bond.

   The first FSN created in PowerStore Manager on node A would be named BaseEnclosure-NodeA-FSN0.

   The same FSN is configured on the opposite node. For example, if you configured the FSN on node A, the same FSN would be configured on node B.

7. Create a NAS server with the Fail-Safe Network.

   The Fail-Safe Network is applied to the NAS server while creating the NAS server in PowerStore Manager. See Create a NAS server for NFS file systems.

Creating NFS exports

Complete the following before you can create NFS exports in PowerStore:

1. Create NAS servers with NFS protocol
2. Create a file system for NFS exports

Documentation resources

See the following for additional information:

Table 1. Documentation resources

Document	Description	Location
PowerStore T and Q Networking Guide for Storage Services	The document provides network planning and configuration information.	dell.com/powerstoredocs
PowerStore Configuring SMB Guide	The document provides information necessary to configure SMB shares with PowerStore Manager.	
PowerStore File Capabilities White Paper	The document discusses the features, functionality, and protocols supported by Dell PowerStore file architecture.	
PowerStore Online Help	Online Help provides context-sensitive information for the page that is opened in PowerStore Manager.	Embedded in PowerStore Manager

2

Create NAS servers

This chapter contains the following information:

Topics:

Overview of configuring NAS servers

Before you can provision file storage on the storage system, a NAS server must be running on the system. A NAS server is a file server that uses the SMB protocol, NFS protocol, or both to share data with network hosts. It also catalogs, organizes, and optimizes read and write operations to the associated file systems.

This document describes how to configure a NAS server with NFS protocol, on which file systems with NFS exports can be created.

Create a NAS server for NFS file systems

You create NAS servers before creating file systems.

Be sure to have your NAS network information available.

1. Select **Storage** > **NAS Servers**.
2. Select **Create**.
3. Continue to work through the **Create NAS Server** wizard.

Wizard Screen	Description
Details	• NAS Server name • NAS Server Description • Network interface - Select a Link Aggregation Group or Fail-Safe Network (see Create the network interface for NAS traffic). **NOTE:** If you select a Fail-Safe Network (FSN), the primary network cannot be modified once a NAS server has been configured using the FSN. • Network information **NOTE:** You cannot reuse VLANs that are being used for the management and storage networks.
Sharing Protocol	**Select Sharing Protocol** Select NFSv3, or NFSv4, or both. **NOTE:** If you select SMB and an NFS protocol, you automatically enable the NAS server to support multiprotocol. For details on multiprotocol file sharing, see *Dell PowerStore Configuring Multiprotocol File Sharing* at PowerStore Documentation page. **Unix Directory Services** (Naming Services) You can configure the naming services with a combination of Local Files and NIS, or LDAP.

Wizard Screen	Description
	See the following sections for configuring: • Using Local Files • With NIS • With LDAP You can choose to enable Secure NFS here. Secure NFS requires the following: • At least one NTP server must be configured on the PowerStore appliance to synchronize the date and time. It is recommended that you set up a minimum of two NTP servers per domain to avoid a single point of failure. • A UNIX Directory Service (UDS) • One or more DNS servers • Either an AD or custom realm must be added for Kerberos authentication • A keytab file must be uploaded to your NAS server when using a custom realm in a Kerberos configuration **DNS** DNS server information is mandatory when: • Joining an AD domain, but optional for a stand-alone NAS server. • Configuring Secure NFS. DNS can also be used to resolve hosts defined on NFS export access lists.
Protection Policy	Optionally, select a protection policy from the list.
File QoS Policy	Optionally, select a file QoS policy from the list.
Summary	Review the content and Select **Previous** to go back and make any corrections.

4. Select **Create NAS Server** to create the NAS server.
   The **Status** window opens, and you are redirected to the **NAS Servers** page once the server is listed on the page.

Once you have created the NAS server for NFS, you can continue to configure the server settings.

If you enabled Secure NFS, you must continue to configure Kerberos.

Select the NAS server to continue to configure, or edit the NAS server settings.

NOTE: When there is a remote system connection, it may take up to 15 minutes for NAS server configuration changes to be reflected on the remote NAS server.

Configure NAS server naming services

You can configure or modify the naming services for a NAS Server.

Naming Services include configuring one or more of the following:

- DNS
- NIS for Unix Directory Services (UDS)
- LDAP for UDS
- Local Files

Configure DNS

You can disable DNS, or enable and configure a NAS server to use DNS.

DNS can also be used to resolve hosts defined on NFS export access lists.

DNS is required for:

- Secure NFS

- Joining an AD domain.

You cannot disable DNS for NAS servers that are configured with:

- Multiprotocol file sharing
- SMB file sharing that is joined to an Active Directory (AD)
- Secure NFS

1. Select **Storage** > **NAS Servers** > **[nas server]** > **DNS**.
2. Enable or disable DNS. If you enabled DNS, enter the DNS server information.

Configure the NAS server UNIX Directory Service for NIS

You can configure NAS server UNIX Directory Service (UDS) for NIS.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** card.
2. If **Disabled** is on, slide the button to change to **Enabled**.
3. In the **Unix Directory Service** drop down, select **NIS**.
4. Enter an NIS **Domain** and add the IP **Addresses** for the NIS servers.
5. Select **Apply**.

To troubleshoot issues with configuring a UDS using NIS, ensure that the NIS server domain and server IP addresses you enter are correct.

Configure a NAS server UNIX Directory Service using LDAP

You can configure a NAS server UNIX Directory Service (UDS) using LDAP.

LDAP must adhere to the IDMU, RFC2307, or RFC2307bis schemas. Some examples include AD LDAP with IDMU, iPlanet, and OpenLDAP. The LDAP server must be configured properly to provide UIDs for each user. For example, on IDMU, the administrator must go in to the properties of each user and add a UID to the UNIX Attributes tab.

You can configure LDAP to use anonymous, simple, and Kerberos authentication. If using Kerberos authentication, you must configure the following before you continue to configure LDAP with Kerberos:

1. From the **Naming Services** card, configure the DNS server that is used to join and unjoin a Kerberos server to a realm.
2. From the **Security** card, add the Kerberos Realm.
1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **UDS** card.
2. If **Disabled** is on, slide the button to change to **Enabled**.
3. In the **Unix Directory Service** drop down, select **LDAP**.
4. Leave the default or enter a different **Port Number**.

   NOTE: By default, LDAP uses port 389, and LDAP over SSL (LDAPS) uses port 636.

5. Add the IP addresses for the LDAP servers.

   The NAS server can be configured to use the DNS service discovery to automatically obtain LDAP server IP addresses.

   NOTE: For this discovery process to work, the DNS server must contain pointers to the LDAP servers, and the LDAP servers must share the same authentication settings.

6. Configure the LDAP authentication as described in the following table:

Option	Description
Anonymous	Specify the Base DN, and the Profile DN for the iPlanet/OpenLDAP server.

Simple	Specify the following:
	• If using AD, LDAP/IDMU:
	  ○ Bind DN in LDAP notation format; for example, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**.
	  ○ Base DN, in the X.509 format (for example, **dc=svt,dc=lab,dc=com**).
	  ○ Profile DN.

Option	Description
	• If using the iPlanet/OpenLDAP server: ○ Bind DN in LDAP notation format; for example, **cn=administrator,cn=users,dc=svt,dc=lab,dc=com**. ○ Password ○ Base DN. For example, if using **svt.lab.com**, the Base DN would be **DC=svt,DC=lab,DC=com**. ○ Profile DN (optional) - For the iPlanet/OpenLDAP server.
Kerberos	Configure a custom realm to hover over any type of Kerberos realm (Windows, MIT, Heimdal). With this option, the NAS Server uses the custom Kerberos realm that is defined in the Kerberos subsection of the NAS server **Security** tab. **NOTE:** If you use NFS secure with a custom realm, you have to upload a keytab file.

7. Select **Retrieve Current Schema** to download the ldap.conf file.
8. Edit and save the `ldap.conf` file.
9. Select **Upload New Schema** to upload the updated `ldap.conf` file.
10. Optionally, enable LDAP Secure (Use SSL), and upload the CA certificate.

To troubleshoot issues with configuring a UDS using LDAP, ensure that:

- The LDAP configuration adheres to one of the supported schemas, as described earlier in this topic.
- The containers that are specified in the `ldap.conf` file hover over containers that are valid and exist.
- Each LDAP user is configured with a unique UID.

Configure NAS server to use local files for naming services

You can configure your naming services to use local files.

- Local files can be used instead of, or also with DNS, LDAP, and NIS directory services.
- If you configure local files with a UNIX Directory Service (UDS), the storage system queries the local files first.
- After you finish creating the NFS server, you can go back and upload more local files.
- Once the NAS server is created, enable the local files as described in the following steps:

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Naming Services** > **Local Files**.
2. For each type of local file, select the down arrow to download the current file. If there is no file on the storage system, the system downloads a file template.
3. Update the file with your system information.

   To use local files for FTP access, the `passwd` file must include an encrypted password for the users. This password is used for FTP access only. The `passwd` file uses the same format and syntax as a standard UNIX system, so you can apply the password to generate the local `passwd` file. On a UNIX system, use `useradd` to add a user and `passwd` to set the password for that user. Then, copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server.
4. Save the updated file to your local machine.
5. Select **Upload Local Files** and browse to the location of the file you edited and select the file to upload.
6. Repeat for each type of file.

To troubleshoot issues with configuring local files, ensure that:

- The file is created with the proper syntax. (Six colons are required for each line.) Reference the template for more details about the syntax and examples.
- Each user has a unique name and UID.

Configure NAS server sharing protocols

You can configure or modify the sharing protocols that are configured for a NAS server.

Configuring sharing protocols for NFS includes setting up one or more of the following:

- NFS Server
- FTP

Configure NFS server

Configure the NAS server for UNIX-only systems, or modify the NFS server settings.

DNS and NTP must be configured before configuring a Secure NFS server.

1. Select the **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **NFS Server** tab.
2. Enable the **Linix/UNIX shares** option to define the NAS server for UNIX support.
3. Enable either **NFSv3**, **NFSv4**, or both.
4. Optionally, disable, or enable Secure NFS.
   Extended UNIX credentials are also enabled.
5. **Enable or disable Extend Unix** credentials.

   NOTE: Secure NFS supports NFS credentials with more than 16 groups, which is equivalent to the extended UNIX credentials option.

   - If this field is selected, the NAS server uses the User ID (UID) to obtain the primary Group ID (GID) and all group GIDs to which it belongs. The NAS server obtains the GIDs from the local password file or UDS.
   - If this field is cleared, the UNIX credential of the NFS request is directly extracted from the network information that is contained in the frame. This method has better performance, but it is limited to including up to only 16 group GIDs.
6. In the **Credential Cache Retention**, enter a time period (in minutes) for which access credentials are retained in the cache.
7. **Apply** the changes.

Configure FTP, or SFTP sharing protocol

You can configure FTP or FTP over SSH (SFTP) settings for an existing NAS server only.

Passive mode FTP is not supported.

FTP access can be authenticated using the same methods as NFS. Once authentication is complete, access is the same as NFS for security and permission purposes. If the format is anything other than `user@domain` or `domain\user`, NFS authentication is used. NFS authentication uses local files, LDAP, NIS, or local files with LDAP or NIS.

To use local files for NFS, FTP access, the `passwd` file must include an encrypted password for the users. This password is used for FTP access only. The `passwd` file uses the same format and syntax as a standard Unix system, so you can leverage this to generate the local `passwd` file. On a Unix system, use `useradd` to add a new user and `passwd` to set the password for that user. Then, copy the hashed password from the `/etc/shadow` file, add it to the second field in the `/etc/passwd` file, and upload the `/etc/passwd` file to the NAS server. See Configure NAS server to use local files for naming services for details on uploading the `/etc/passwd` file.

1. Select the **Storage** > **NAS Servers** > **[nas server]** > **Sharing Protocols** > **FTP** tab.
2. Under **FTP**, if Disabled in on, slide the button to **Enable**.
3. Optionally also enable SSH FTP. Under **SFTP**, if Disabled in on, slide the button to **Enable**.
4. **Under FTP/SFTP Server Access**, Select which type of authenticated users have access to the files.
5. Optionally, show the **Home Directory and Audit** options.
   - Select or clear the **Home directory restrictions**. If disabled, enter the **Default home directory**.
   - Select or clear **Enable FTP/SFTP Auditing**. If checked, enter the directory location of where to save the audit files, and the maximum size allowed for the audit file.
6. Optionally, **Show Messages**, and enter a default **Welcome message**, and **Message of the day**.
7. Optionally, **Show Access Control List** to provide access or deny access to **Filtered Users**, **Filtered Groups**, and **Filtered hosts**.
8. Click **Apply**.

Configure Kerberos for NAS server security

You can configure the NAS Server with Kerberos.

Kerberos is a distributed authentication service designed to provide strong authentication with secret-key cryptography. It works on the basis of "tickets" that allow nodes communicating over a non-secure network to prove their identity in a secure

manner. When configured to act as a secure NFS server, the NAS server uses the RPCSEC_GSS security framework and Kerberos authentication protocol to verify users and services.

If the NAS server has been configured with NFS only, and you are configuring Secure NFS, or LDAP with Kerberos, you must configure Kerberos with a custom realm before configuring security in PowerStore.

If the NAS server has been configured with both the NFS and SMB protocol, you have the option of using Kerberos that is inherited with AD since the domain joined SMB server exists on the NAS server.

The storage system must be configured with an NTP server. Kerberos relies on the correct time synchronization between the KDC, servers, and client on the network.

Configuring Kerberos for Secure NFS

If you are configuring Kerberos for Secure NFS, be aware of the following:

- If configuring the NAS server for NFS only, you must configure the NAS server with a custom realm. If you have configured the NAS server with NFS and SMB, you can use either the AD or custom realm.
- Using LDAPS or LDAP with Kerberos is recommended for increased security.
- A DNS server must be configured at the NAS-server level. All members of the Kerberos realm, including the KDC, NFS server, and NFS clients, must be registered in the DNS server.
- The NFS client's hostname FQDN and NAS server FQDN must be registered in the DNS server. Clients and servers must be able to resolve any member of the Kerberos realm's FQDNs to an IP address.
- The FQDN part of the NFS client's SPN must be registered in the DNS server.
- A keytab file must be uploaded to your NAS server when configuring Secure NFS.

Create a custom realm for Kerberos

You can configure a custom realm to use with Kerberos.

A custom Kerberos realm lets you configure any kind of KDC (MIT/Heidmal or AD). Use this method when you do not have an SMB server domain that is configured on the NAS server or if you want to use a different Kerberos realm than the realm configured for the SMB server.

Create custom realm for pure NFS server

To use a UNIX-based KDC, follow these steps before configuring Kerberos in PowerStore. The steps assume that you want to use myrealm in the Kerberos realm linux.dellemc.com as the hostname of the NFS server.

1. Run the `kadmin.local` tool.
2. Create the principals and their keys:

   ```
   kadmin.local: addprinc -randkey nfs/myrealm.linux.dellemc.com
   ```

   and/or

   ```
   kadmin.local: addprinc -randkey nfs/myrealm
   ```

3. Put the key of the principal into the keytab file myrealm.linux.dellemc.fr:

   ```
   kadmin.local: ktadd -k myrealm.linux.dellemc.com.keytab nfs/myrealm.linux.dellemc.fr
   ```

Create custom realm for multiprotocol (NFS and SMB) NAS server

To use a Windows-based KDC without using the SMB server account on the NAS server, follow these steps before configuring Kerberos in PowerStore. The steps assume that you want to use myrealm.windows.dellemc.com as the FQDN for the NFS server.

1. Create account myrealm for the NAS server in the Active Directory (AD) of the windows domain windows.dellemc.com.

2. Register the service SPN on the computer account that you created:

```
C:\setspn -S nfs/myrealm.windows.dellemc.com myrealm
```

3. Verify that the SPN was created.

```
C:\setspn myrealm
```

4. Generate a keytab file for the SPN:

```
C:\ktpass -princ nfs/myrealm.windows.dellemc.com@WINDOWS.DELLEMC.COM -mapuser
WINDOWS\myrealm
 -crypto ALL +rndpass -ptype KRB5_NT_PRINCIPAL -out myrealm.windows.dellemc.com.keytab
```

Configure Kerberos security for the NAS server

You can configure the NAS server with Kerberos security.

If configuring for NFS, DNS and UDS must be configured for the NAS server and all members of the Kerberos realm must be registered in the DNS server.

If using a NAS server that is configured for both SMB and NFS, be sure to add the SMB server to the AD domain.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Security** > **Kerberos**.
2. If Disabled is on, slide the button to change to **Enabled**.
3. Enter the name of the **Realm**.
4. Enter the **Kerberos IP Address** and click **Add**.
5. Enter the TCP Port for Kerberos to use. 88 is the default port.
6. Click **Apply**.

If you choose to change from an AD realm to a custom realm after the NAS server is successfully created with Secure NFS, you cannot mount any NFS exports until you perform the following operations:

1. Create a Keytab file.
2. Remove the AD realm from the NAS server.
3. Enter the Username and Password for the AD Server.
4. Enter the custom realm.
5. Upload the Keytab file.

3

Configure NFS exports

This chapter contains the following information:

Topics:

File systems and NFS exports overview

While creating File Systems and NFS Exports, it is helpful to note the following:

- A NAS server must be configured to support NFS protocol before creating a file system.
- You can choose to add NFS Exports the first time you create the file system, or you can add NFS Exports to a file system after it has been created.

Create a file system for NFS exports

You can create a file system for NFS exports.

Ensure that there is a NAS server that is configured to support the NFS protocol.

1. Select **Storage** > **File Systems**.
2. Click **Create**.
   The **Create File System** wizard launches.
3. Select **General** or **VMware File System** as the file system type.

   NOTE: VMware file system is a PowerStore file system that is optimized for VMware and used for VMware workloads. This option should be selected only for VMware NFS datastores. For all other file systems, select **General**.

4. Select an NFS enabled NAS server for the file system.
5. Specify the file system details, including the file system name and size, minimum size is 3 GB, maximum size is 256 TB.

   NOTE: All thin file systems, regardless of size, have 1.5 GB reserved for metadata upon creation. For example, after creating a 100 GB thin file system, PowerStore T model and PowerStore Q model show 1.5 GB used. When the file system is mounted to a host, it shows 98.5 GB of usable capacity. This is because the metadata space is reserved from the usable file system capacity.

6. Optionally, select file-retention type (available for general file systems only):
   - Enterprise (FLR-E) - Protects content from changes that users make through NFS and FTP. An administrator can delete an FLR-E file system that contains protected files.
   - Compliance (FLR-C) - Protects content from changes that are made by users and administrators and complies with SEC rule 17a-4(f) requirements. FLR-C file system can be deleted only when it does not contain any protected files.

   NOTE: FLR state and file-retention type are set at file system creation and cannot be modified.

   Set the retention periods:
   - Minimum - Specifies the shortest period for which files can be locked (default value is 1 day).
   - Default - Used when a file is locked and no retention period is specified.
   - Maximum - Specifies the longest period for which files can be locked.
7. Optionally, configure the initial export for the file system.

NOTE: You can add NFS exports to the file system later.

8. If you configured initial export, configure Host Access.

Option	Description
Minimum Security	Select **Sys** to allow users with non-secure NFS, or Secure NFS to mount and NFS export on the file system. If you are not configuring Secure NFS you must select this option. If you are creating a file system with Secure NFS, then you can choose from the following options: • **Kerberos** to allow any type of Kerberos security for authentication (krb5/krb5i/krb5p). • **Kerberos with Integrity** to allow both Kerberos with integrity and Kerberos with encryption security for user authentication (krb5i/krb5p). • **Kerberos with Encryption** to allow only Kerberos with encryption security for user authentication (krb5p).
Default Access	The type of access that is applied to the hosts by default. Optionally, you can choose a different type of access to the host when adding individual hosts. Options include: • **No Access**—No access is permitted to the storage resource or share. • **Read/Write**—Hosts have permission to read and write to the NFS datastore or share. • **Read-Only**—Hosts have permission to view the contents of the storage resource or share, but not to write to it. **NOTE:** ESXI hosts must have **Read//Write** access in order to mount an NFS datastore using NFSv4 with **Kerberos NFS owner** authentication. • **Read/Write, allow Root**—Hosts have permission to read and write to the storage resource or share, and to grant revoked access permissions (for example, permission to read, modify, and run specific files and directories) for other login accounts that access the storage. The root of the NFS client has root access to the share. **NOTE:** Unless the hosts are part of a supported cluster configuration, a void granting Read/Write access to more than one host. **NOTE:** ESXi hosts must have **Read/Write, allow Root** access in order to mount an NFS datastore using NFSv4 with NFS Owner:root authentication. • **Read-Only, allow Root** — Hosts have permission to view the contents of the share, but not to write to it. The root of the NFS client has root access to the share.
Add Host	Enter hosts individually, or you can add hosts by uploading a properly formatted CSV file. You can download the CSV file first to obtain a template. To download, edit, and use a CSV file template: a. Click the **Export Hosts** icon. b. Update the CSV file with the hosts, and access types you want to import. c. Save the CSV file to your local machine. d. Click **Import CSV file**. e. Browse to the CSV file, and click **Open** in your Microsoft File Explorer window. The hosts from the CSV file appear in the **Import Host List** with the **Access Type** you defined in the CVS file.

9. Optionally, add a protection policy to the file system.
   If you are adding a protection policy to the file system, the policy must have been created before creating the file system. The selected protection policy can include both snapshot and replication rules.
10. Optionally, add a QoS policy to the file system.

    NOTE: If the selected policy sets a bandwidth that exceeds the maximum bandwidth set for the NAS server, then the effective bandwidth is the maximum bandwidth of the server.

11. Review the summary and click **Create File System**.
    The file system is added to the **File System** tab. If you created an export simultaneously, the export displays in the **NFS export** tab.

Create an NFS export

You can create an NFS export on a file system.

1. Select the **Storage** > **File Systems** > **NFS Export** tab.
2. Click **Create**.
   The **Create NFS Export** wizard launches.
3. Enter the requested information while noting the following:
   - If you want to create an export based on a snapshot, then the snapshots must be created before creating the NFS export.
   - **Local Path** must correspond to an existing folder name within the file system that was created from the host-side.
   - The value specified in the **NFS Export Details**, **Name** field, along with the NAS server IP, constitutes the export path.

     NOTE: You can also mount the export using the NAS server IP and local path.

   - NFS export names must be unique at the NAS server level per protocol. However, you can specify the same name for an SMB share, and NFS exports.
4. Once you approve the settings, click **Create NFS Export**.
   The NFS Export displays on the **NFS Export** page.

File-level retention

File-level retention (FLR) enables you to prevent modifications or deletion of locked for a specified retention period. Protecting a file system using FLR enables you to create a permanent, and unalterable set of files and directories. FLR ensures data integrity and accessibility, simplifies archiving procedures for administrators and improves storage management flexibility.

There are two levels of file-level retention:

- Enterprise (FLR-E) - Protects data from changes that are made by users and storage administrators using SMB, NFS, and FTP. An administrator can delete an FLR-E file system which includes locked files.
- Compliance (FLR-C) - Protects data from changes that are made by users and storage administrators using SMB, NFS, and FTP. An administrator cannot delete an FLR-C file system which includes locked files. FLR-C complies with SEC rule 17a-4(f).

The following restrictions apply:

- File-level retention is available on unified PowerStore system 3.0 or later.
- FLR is not supported in VMware file systems.
- Enabling a file-level retention for a file system and the level of FLR are set at file system creation time and cannot be modified.
- FLR-C does not support restoring from a snapshot.
- When refreshing using a snapshot, both file systems must be of the same FLR level.
- When replicating a file system, source and destination file systems must be of the same FLR level.
- A cloned file system has the same FLR level as the source (cannot be modified).

The FLR mode is displayed in the **File Systems** screen.

Configure DHSM server

File-level retention requires DHSM server credentials.

DHSM server is also required for Window hosts that want to use FLR and are required to install FLR toolkit that enables managing FLR-enabled file systems.

1. Select **Storage** > **NAS Servers** > **[NAS server]** > **Protection** > **DHSM**.
2. If disabled, slide the button to **Enabled**.
3. Enter the user name and password for the DHSM server and verify the password.
4. Select **Apply**.

Configure file-level retention

File-level retention is configured at file system creation. For details, see Create file system.

NOTE: Retention period parameters can be modified at a later time.

Modify file-level retention

Retention period parameters can be set at file system creation or later and can be modified. Modifying retention period parameter does not affect files that are already locked.

1. Select **Storage** > **File Systems** > **[file system]** > **Security & Events** > **File-Level Retention**.
2. Set the retention period parameters:
   - Minimum retention period - Specifies the shortest period for which an FLR-enabled file system can be protected (default value is one day).
   - Default retention period - Used when a file is locked and a retention period is not specified (default value is one year).
   - Maximum retention period - Specifies the longest period for which an FLR-enabled file system can be protected (default value is infinite).
3. Optionally, set the advanced settings:
   - Automatic file locking - You can specify whether to automatically lock files in an FLR-enabled file system and set a policy interval that determines the time period between file modification and automatic lock (policy interval default value is one hour).
   - Automatic file deletion - You can specify whether to automatically delete locked files after their retention period is expired. The first scan for locating files for deletion is seven days after the feature is enabled.
4. Select **Apply**.

4

More NAS server features

This chapter contains the following information:

Topics:

Set the preferred UNIX Directory Service

After you have created a NAS server, you can set the preferred UNIX Directory Services (UDS) search order for user access.

1. Select **Storage** > **NAS Servers**.
2. Select the checkbox in the **Name** column to the left of the NAS server.
3. Click **Modify**.
4. Select the preferred UDS search order for use from the list of **Unix Directory Service Search Order** drop down.
5. Click **Apply**.

Configure NAS server networks

You can modify or configure NAS server networks.

Configure the following for NAS server networks:

- The file interfaces
- Routes to external services such as hosts.

Configure file interfaces for a NAS server

You can configure the file interfaces for a NAS server after the server has been added to PowerStore.

You can add more file interfaces, and define which is the preferred interface to use. Also, you can define which interface to use for production and backup, or for IPv4, or IPv6.

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. On the **Network** page, click **Add** to add another file interface to the NAS server.
3. Enter the File Interface properties.

   NOTE: Do not reuse VLANs that are being used for the management and storage networks.

4. You can perform the following on a File Interface by selecting a file interface from the list. Select:

Option	Description
Modify	To change the properties of the file interface properties.
Delete	To delete the file interface from the NAS server.
Ping	To test the connectivity from the NAS server to the external IP address.
Preferred Interface	To define which interface PowerStore should default to using when multiple production and backup interfaces have been defined.

Configure routes for the file interface for external connections

You can configure the routes that the file system uses for external connections.

You can use the **Ping** option from the **File Interface** card to determine if the file interface has access to the external resource.

Usually, the NAS server interfaces are configured with a default gateway, which is used to route requests from the NAS server interface to external services.

Use the following steps:

- If you must configure more granular routes to external services.
- To add a route to access a server from a specific interface through a specific gateway.

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Network** > **Routes to External Services**.
2. Click **Add** to enter the route information in the **Add Route** wizard.

Enable NDMP backup

You can configure standard backup for the NAS servers using NDMP. The Network Data Management Protocol (NDMP) provides a standard for backing up file servers on a network. When NDMP is enabled, a third-party Data Management Application (DMA), such as Dell Networker, can detect the PowerStore NDMP using the NAS server IP address.

Enabling NDMP is performed after the NAS server is created.

PowerStore supports:

- Three-way NDMP - The data is transferred through the DMA over a local area network (LAN) or Wide Area Network (WAN).
- Full and incremental backups

1. Select **Storage** > **NAS Servers** > **[nas server]** > **Protection** .
2. Under **NDMP Backup**, if **Disabled** is on, slide the button to change to **Enabled**.
3. Enter a password for the **New Password**.
   The username is always `ndmp`.
4. Reenter the same password as the new password in **Verify Password**.
5. Click **Apply**.

Leave the NDMP page, and return back to the NDMP page to validate that NDMP is enabled.

5

More file system features

This chapter contains the following information:

Topics:

File system quotas

You can track and limit drive space consumption by configuring quotas for file systems at the file system or directory level. You can enable or disable quotas at any time, but it is recommended that you enable or disable them during non-peak production hours to avoid impacting file system operations.

NOTE: You cannot enable quotas for read-only file systems.

NOTE: Quotas are not supported in VMware file systems.

NOTE: When you create a replication session, quotas are not visible on the destination system even if they are enabled on the source system.

Types of quotas

There are three types of quotas that you can put on a file system.

Table 2. Quota types

Type	Description
User Quotas	Limits the amount of storage that an individual user consumes by storing data on the file system.
Tree Quota	Tree quotas limit the total amount of storage that is consumed on a specific directory tree. You can use tree quotas to: ● Set storage limits on a project basis. For example, you can establish tree quotas for a project directory that has multiple users sharing and creating files in it. ● Track directory usage by setting the tree quota hard and soft limits to 0 (zero). **NOTE:** If you change the limits for a tree quota, the changes take effect immediately without disrupting file system operations.
User quota on a quota tree	Limits the amount of storage that an individual user consumes by storing data on the quota tree.

Quota limits

Table 3. Hard and soft limits

Type	Descriptions
Hard	A hard limit is an absolute limit on storage usage. If a hard limit is reached for a user quota on a file system or quota tree, the user cannot write data to the file system or tree until more space becomes available. If a hard limit is reached for a quota tree, no user can write data to the tree until more space becomes available.

Table 3. Hard and soft limits (continued)

Type	Descriptions
Soft limit	A soft limit is a preferred limit on storage usage. The user is allowed to use space until a grace period has been reached. The user is alerted when the soft limit is reached, until the grace period is over. After that, an out of space condition is reached until the user gets back under the soft limit.

Quota grace period

The Quota grace period enables you to set a specific grace period to each tree quota on a file system. The grace period counts down the time between the soft and hard limit, and alerts the user about the time remaining before the hard limit is met. If the grace period expires you cannot write to the file system until more space has been added, even if the hard limit has not been met.

You can set an expiration date for the grace period. The default is 7 days, alternatively you can set the grace period expiration date to an infinite amount of time (the grace period never expires), or for a specified number of days, hours or minutes. Once the grace period expiration date is met, the grace period no longer applies to the file system directory.

Additional information

For more information about quotas, see the *Dell PowerStore File Capabilities White Paper*.

Enable user quotas

You must enable quotas and set the user quota defaults before you can add a user quota to a file system.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas**.
2. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Properties**.
3. Slide the **Disabled** button to **Enabled**.
4. Enter the default **Grace Period** for the user quota on the file system which will count down the time after the soft limit is met until the hard limit is met.
5. Enter a default **Soft Limit**, and a default **Hard Limit** and click **Update**.

Add a user quota onto a file system

Create a user quota on a file system to limit or track the amount of storage space that individual users consume on that file system. When you create or modify user quotas, you can use default hard and soft limits that are set at the file-system level.

You must enable Quotas and set the User Quota defaults before you can add a User Quota to a files system. See Enable User Quotas.

NOTE: You cannot create quotas for read-only file systems.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **User**.
2. Select **Add** on the **User Quota** page.
3. In the **Add User Quota** wizard, provide the requested information. To track space consumption without setting limits, set **Soft Limit** and **Hard Limit** to 0, which indicates no limit.
4. Select **Add**.

Add a quota tree onto a file system

Create a quota tree at the directory level of a file system to limit or track the total storage space that is consumed for that directory.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.

2. Select **Add**.
3. Slide the **Enforce User Quota** to the right to enabled User Quota defaults on the Tree Quota.
4. Provide the requested information.
   - Enter a **Grace Period** to count down the time between the soft and hard limit. You will begin to receive alerts once the grace period is reached.
   - To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.
5. Select **Add**.

Add a user quota onto a quota tree

Create a user quota on a quota tree to limit or track the amount of storage space that individual users consume on that tree. When you create user quotas on a tree, you can to use the default grace period and default hard and soft limits that are set at the tree-quota level.

1. Select **Storage** > **File Systems** > **[file system]** > **Quotas** > **Tree Quotas**.
2. Select a path, and click **Add User Quota**.
3. On the **Add User Quota** screen, provide the requested information. To track space consumption without setting limits, set the **Soft Limit** and **Hard Limit** fields to 0, which indicates no limit.

File Quality of Service (QoS)

In a system that is running varying workloads with unpredictable demands, Quality of Service ensures that critical applications can get priority and provides predictable performance for each application.

You can apply Quality of Service (QoS) policies to set maximum bandwidth for NAS servers and file systems.

When you assign a QoS policy to a NAS server or file system, SDNAS enforces the policy on NFS/SMB services.

Bandwidth limits are applied based on NFS/SMB, and SFTP/FTP protocols.

If the set bandwidth exceeds the maximum bandwidth set for the NAS server, then the effective bandwidth is the maximum bandwidth of the server.

NOTE: It may take some time for a QoS policy to take effect.

NOTE: QoS is not supported with NAS server clones, file system clones, snapshots, snapshot clones, and snapshot refresh.

NOTE: Bandwidth applied to NAS servers and file systems as part of an assigned QoS policy can deviate within a margin of 10 percent.

File QoS limits:

- A QoS policy can include one I/O limit rule.
- Up to 100 file QoS policies can be defined.
- Up to 100 file QoS rules can be defined.
- Only one QoS policy can be applied to a NAS server or file system.
- The same QoS policy can be assigned to multiple NAS servers and file systems.

QoS and file replication:

- When the NAS server has a replication rule, the assigned QoS policy is replicated to the destination server.
- When you modify QoS policies that are assigned to the NAS server, the changes are replicated to the destination server.
- It is not possible to modify the replicated QoS policy configuration on the destination server.
- It is not possible to assign a QoS policy to a NAS server or file system on the destination server.
- After assigning a QoS policy to a NAS server or file system on the source server, it is not possible to unassign the policy from the destination server.
- After you unassign a QoS policy from a NAS server, the policy should be unassigned at the destination as well.
- After failover, you can assign, unassign, and modify replicated QoS policies.

File QoS limits

You can create I/O limit rules for NAS servers and file systems. An I/O limit rule defines the allowed maximum bandwidth.

- Each NAS server or file system can be associated with only one limit rule.
- Each policy can include only one rule.
- You can define up to 100 rules.

I/O limit rules apply only to I/O from external hosts, and not to internal asynchronous or synchronous replication operations or migration I/O.

I/O limit rules are not applied to objects that are created internally, such as NDMP backups served by an NDMP server in SDNAS.

Specific alerts for file QoS limits are not supported. To learn if the set limits require an adjustment, you can monitor the Latency, IOPS, and Bandwidth charts for each NAS server and file system.

Create a Quality of Service (QoS) bandwidth limit rule and policy

You can create a bandwidth limit rule and add it to a QoS policy.

1. Select **Storage** > **Quality of Service (QoS)** > **File I/O Limit Rules**.
2. Select **Create**.
3. On the **Create File I/O Limit Rule** slide-out, set the rule name and max bandwidth (MB/s).
4. Select **Create**.
   The rule is added to the File I/O Limit Rules table.
5. Select **File QoS Policies**.
6. Select **Create**.
7. On the **Create File QoS Policy** slide-out, set the policy name. You can also add a description.
8. From the rule list, select the rule that you want to add to the policy.
9. Select **Create**.
   The policy is added to the File QoS Policies table.

Assign a file QoS policy

After you define an I/O limit rule as part of a file QoS policy, you can assign it to a NAS server or a file system. You can also modify the assigned QoS policy.

NOTE: It is also possible to assign a QoS policy as part of the procedure for creating a NAS server or a file system.

1. Select **Storage** > **NAS Servers** or **Storage** > **File Systems**.
2. Select the checkbox next to the relevant NAS server or file system.
3. Select **More Actions** > **Change QoS Policy**.
4. On the **Change QoS Policy** slide-out, select a file QoS policy, and then select **Apply**.
   The policy is assigned. You can view the assigned policy name on the **QoS Policy** column in the NAS Server and File Systems tables. You can view the impact of the assigned policy on performance by selecting **Storage** > **NAS Servers** > **[NAS server]** > **Performance** or **Storage** > **File Systems** > **[file system]** > **Performance**.
   NOTE: You can also set the QoS policy by selecting the relevant NAS server or file system and then selecting **Modify**.

Modify a file QoS policy

You can modify a QoS policy by selecting a different I/O limit rule.

You cannot modify a policy that is assigned to a NAS server or file system.

1. Select **Storage** > **Quality of Service (QoS)**.
2. From the **File QoS Policies** table, select the checkbox next to the QoS policy that you want to modify.
3. Select **Modify**.

4. In the **Modify QoS Policy** window, you can modify the name and description of the policy, and select a different I/O limit rule.
5. Select **Apply**.

NOTE: You can also modify a QoS policy from the storage resource **Properties** screen.

Delete a file QoS policy

Ensure that the QoS policy that you want to delete is not assigned to a NAS server or file system.

1. Select **Storage** > **Quality of Service (QoS)**.
2. From the **File QoS Policies** table, select the QoS policy that you want to delete.
3. Select **More Actions** > **Delete**.
4. Select **Delete** to confirm.

6

NAS server replication

This chapter contains the following information:

Topics:

Overview

To enable enhanced redundancy and recovery if data loss occurs, PowerStore enables you to replicate NAS servers from a local system to a remote system.

By default, replication occurs at a NAS server level - all the file systems within the replicated NAS server are replicated to the remote system. You can select to add file systems or delete file systems from the NAS server when it is a part of a replication session.

You can select asynchronous replication, where the systems are synchronized based on a defined RPO, or synchronous replication, where changes are replicated from the source system to the destination system immediately when they occur.

The following pre-requisites are required to enable file replication:

- A file remote system
- A File Mobility network must be configured and mapped (see *PowerStore T and Q Networking Guide for Storage Services* on the PowerStore Documentation page).
- A protection policy that includes a replication rule.

Consider the following for NAS server replication:

- It is not required to define separate protection policies for NAS servers. The same protection policies can be applied to both block and file replication.
- You can delete file systems from the source system of a replication session. After deletion, only the remaining file systems are replicated to the destination. The status of the destination system is not impacted following the file system deletion. If you delete file systems from a replicating source NAS server and then fail over to the destination system, the file systems that were deleted from the old source are not replicated by the new source. If you want to replicate these file systems, generate clones that can be replicated and delete the file systems.
- You can fail over a replication session to the remote system. Failover occurs for all the file systems within the failed over NAS server.
- When you create a replication session, quotas are not visible on the destination system even if they are enabled on the source system.
- For asynchronous replication, RPO is configured at the NAS server level and is identical across all associated file systems.
- For synchronous replication, increasing the size of a file system that is under replication requires pausing the replication session first. Reducing the size of a file system does not require pausing the replication session.
- For synchronous replication, it is not possible to change the network latency of the replication system pair to a higher value than five milliseconds when synchronous replication sessions are defined.
- Switching between synchronous and asynchronous replication is not supported for file replication.

For detailed information about NAS server replication procedures, see *Protecting your Data* on the PowerStore Documentation page.

Testing disaster recovery for NAS servers under replication

A disaster recovery test performs a disaster recovery plan that enables you to check that the system can recover and restore data and operation if disaster occurs.

PowerStore provides several options to test the ability of the system to recover from a disaster and regain functionality:

- Clone a NAS server for disaster recovery testing using unique IP addresses.
- Clone a NAS server for disaster recovery testing using an isolated network with duplicate IP addresses.
- Perform a planned failover.

Clone a NAS server for disaster recovery testing using unique IP addresses

Cloning a NAS server is the recommended option for testing DR. You can clone the NAS server using the PowerStore Manager and test it without impacting production. To enable access to the newly cloned NAS server, it is required to configure a new and unique network interface. The configured IP address cannot be in use on either the source or destination NAS servers. Unique settings are also required for joining the server to an AD domain.

Changes that are made on the cloned file systems and on production file systems do not impact each other. When the DR test is complete, the cloned server can be deleted.

You can choose one of the following options:

- Clone the NAS server on the source system, replicate it to the destination, and perform a planned failover to the destination system.
- Clone the NAS server on the destination system and access the data (failover is not required because the cloned resources are already accessible on the destination system).

1. In the PowerStore Manager, select **Storage** > **NAS Servers** .
2. Select the NAS server that you want to clone, and then select **Repurpose** > **Clone NAS Server**.
3. In the **Create Clone** window, provide a name for the clone and select the file systems that you want to clone.
4. Select **Create**.
   The cloned NAS server is added to the servers list.
5. Select the cloned NAS server name to open the server details window.
6. To add a file interface:
   a. Select the **Network** tab.
   b. Under **File Interface** select **Add**.
   c. Provide the interface information and select **Add**.
7. To set the sharing protocol:
   a. Select the **Sharing Protocols** tab.
   b. Select the relevant protocol (SMB, NFS, or FTP).
   c. Configure the necessary information and select **Apply**.
8. If you cloned the source NAS server:
   a. Replicate the NAS server to the destination system. For details, see NAS server replication.
   b. Perform a planned failover to the destination. For details see, Planned failover.
   c. Check if the host can access the data.
9. If you cloned the replicated production server on the destination system, failing over is not required. Verify host access.

Clone a NAS server for disaster recovery testing using an isolated network with duplicate IP addresses

It is possible to test disaster recovery using the same configuration as production. Using identical settings may reduce risk and increase reproducibility in a failure scenario. However, using duplicate IP addresses creates conflicts. Running the DR test on an environment that is isolated from the production environment enables you to avoid these conflicts.

In PowerStoreoperating system 3.6 and later, you can create an isolated Disaster Recovery Testing environment (DRT) to help you be prepared for a disaster.

Creating an isolated environment enables you to use the same IP address and hostname as the production system, and perform a DRT for a NAS server under replication without any impact on production.

To create a DRT environment, you must set up an isolated network with a separate DRT router and to create link aggregations with the network I/O ports.

Using PSTCLI or REST API, create a dedicated networking environment on the destination server by cloning the NAS server under replication on the destination PowerStore system. The clone is a full copy of the production environment and a dedicated test environment, which is isolated from production. You can create an isolated networking environment and configure the test environment with the same IP address and hostname as the production system. The DRT NAS server has no impact on the production environment, and can run without IP address conflicts when failover and failback occur on the replication NAS server.

To test DR using an isolated test environment:

1. Create the NAS server clone on the destination. Use the `is_dr_test` flag.
2. Create a user bond interface for NAS using the same IP address as the Source NAS server.
3. Join the clone to the AD (if required).
4. Verify that hosts can access the data.

NOTE: You can also use DRT on stand-alone NAS servers.

Pre-requisites and limitations

To create a DRT environment, ensure that the following requirements are met:

- Acquire the private network information:
  - Gateway
  - Netmask
  - VLAN ID (optional)
- Identify the network ports of the isolated network and the network ports of the production network.

Note the following limitations when creating a DRT environment:

- Bond interface dedicated to DRT cannot be used to create any other production NAS servers.
- A NAS server that is configured as production cannot be reconfigured as part of the DRT.
- A NAS server that is configured as part of the DRT cannot be reconfigured as production.
- A NAS server that is no longer a part of a DRT cannot be reconfigured, and must be deleted.
- After a NAS server is active and configured with network information, additional configuration (such as DNS, CAVA, and Kerberos) should be done manually.
- DRT-enabled NAS server cannot be replicated.
- Modifying and deleting the NAS server can be done using the PowerStore Manager.

Configure the disaster recovery test environment using PSTCLI

1. Acquire the name of the NAS server on the destination site (to be cloned):

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server show
# | id | name | operational_status |  current_node_id  | file_interfaces.ip_addre~
--+-------------+--------+--------------------+-------------------
1 |647f545a-4b11-5cdd-4d4c-eeeba81eb143 | File80| Started | R2C4-appliance-1-node~|
127.1.1.1
```

2. Clone the NAS server by providing a new name for the clone and using the `-is_dr_test true` switch:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> nas_server -name File80
clone -name File80_c -is_dr_test true
Success
```

3. Find the IP port ID for the NAS File Bond that is connected to the isolated network:

   NOTE: If the NAS File Bond was not created, you can create it using PSTCLI or PowerStore Manager.

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> ip_port_show -output nvp
8:  id =IP_PORT23
    current_usages =
    ip_pool_addresses =
```

```
    bond:
    name=BaseEnclosure-NodeA-bond1
```

4. Create the file interface for the cloned NAS server:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface create
-nas_server_name File80_c -ip_address "10.10.10.10" -prefix_length 24 -gateway
"10.10.10.1" -vlan_id 5
-ip_port_id IP_PORT23
Created
# |     id
--+------------------------------------
1 |64830ae5-2760-59ce-4c90-82772509648e
```

5. View file interface:

```
[SVC:service@9CB0BD3-B user]$ pstcli -d <PowerStore_IP> file_interface_show
# |id | nas_server_id | ip_address | prefix_length | gateway | is_disabled
--+-------------+--------+--------------------+-------------------
  1 |647f5509-11f4-a52d-ee1f-82772509648e | 647f545a-4b11-5cdd-4d4c-eeeba81eb143 |
10.10.10.10 |24 | 10.10.10.1 | no
  2 |64830ae5-2760-59ce-4c90-82772509648e | 6483092f-3e71-8a92-0a0b-82772509648e |
10.10.10.10 |24 | 10.10.10.1 | no
```

Configure a NAS server in a DRT environment using REST API

NOTE: If you are not using REST API, skip this section.

1. To clone the NAS server in the specified namespace, run `/nas_server/{id}/clone`, and specify `is_dr_test` as true.
2. To create a network interface, run `/file_interface` and specify the private network parameters.

   NOTE: This step creates the file interface for the cloned NAS server using the same IP address, netmask, and gateway as the production NAS server. Use the bond interface/IP_Port that is associated with the private network.

The NAS server is up and can be used for DRT in the isolated network.

Perform a planned failover

You can use planned failover to test disaster recovery. When you perform a planned failover, the NAS server replication session is manually failed over from the source system to the destination system. Before the failing over, the destination system is synchronized with the source system, to prevent any data loss.

NOTE: Failing over the production NAS server to the destination system may impact production.

Before performing a planned failover, be sure to stop I/O operations for any applications and hosts. You cannot pause a replication session that is undergoing a planned failover.

When operation is normal, changes made to the NAS server and file systems during the DR test are preserved and replicated back to the original source when reprotect is initiated (either manually or automatically). However, if you do not want to save the changes made during DR testing (either data or configuration), you can select to discard the changes, using REST API or PSTCLI commands:

- REST API - `POST /replication_session/{id}/reprotect discard_changes_after_failover`
- PSTCLI - `replication_session -id <value> reprotect [-discard_changes_after_failover]`

The changes that are discarded:

- For NAS Servers:
  - Configuration changes
- For file systems:
  - Configuration changes
  - File system data changes
  - Snapshot resources

    - File system size changes
    - Quota changes
- For exports and shares:
    - NFS export changes
    - SMB share changes

NOTE: This option is only supported for asynchronous replication.

For details on using the REST API and CLI to discard changes after failover, see *Dell PowerStore REST API Reference Guide* and *Dell PowerStore CLI Reference Guide* at dell.com/powerstoredocs.

After the NAS server is reprotected, you can initiate a planned failover again to bring the resources online on the original source system.

NOTE: Do not perform unplanned failover for disaster recovery purposes. Unplanned failover should be used only when the source system is inaccessible.

There are two ways to initiate a planned failover:

- From **Protection** > **Replication**, select the relevant replication session, and then select **Planned Failover**.
- From the **Protection** tab of the resource, select **Replication**, and then select **Planned Failover**.

After a planned failover, the replication session is inactive. To synchronize the destination storage resource and resume the replication session, use the **Reprotect** action. You can also select the auto-reprotect option before failing over, which automatically initiates the synchronization in the opposite direction (at the next RPO) after the failover is complete, and returns the source and the target system to a normal state.

NOTE: After failover, user quotas are not visible on the destination system (which has become the new source). To view the user quotas, manually refresh the quotas by selecting **Storage** > **File Systems**, checking the checkbox next to the relevant file system, and then selecting **More Actions** > **Refresh Quotas**.

Network disconnection during DRT

When performing DRT, it is not recommended to simulate a network failure between the local and remote systems, and then perform an unplanned failover to the destination system to enable access to the DR NAS server. Since there is no communication between the systems, PowerStore cannot ensure that both NAS servers are in a compatible state. After connection is restored, both NAS servers are in production mode (split brain). As a result, both systems switch to maintenance mode to prevent data from being written to both locations.

To resolve this state, Technical Support intervention is required.

For more information, see Dell Knowledge Base Article 000215482 (Cutting the network connection between sites...).

7

Using CEPA with PowerStore

This chapter contains the following information:

Topics:

Events publishing

CEE enables third-party applications to receive event information from the storage system upon accessing file systems.

The Common Event Enabler (CEE) provides an event publishing solution for PowerStore clients that allow third-party applications to register and receive event notification and context from the storage system when accessing file systems. Receiving event notification enables you to take event-driven actions on the storage to prevent security threats such as ransomware or unauthorized access.

The CEE Common Events Publishing Agent (CEPA) consists of applications that are designed to process SMB and NFS files and directory event notifications. The CEPA delivers both event notification and associated context to the application in one message. Context can consist of file metadata or directory metadata that is needed for business policy decisions.

To enable CEE CEPA support, you must enable CEE CEPA and create an Event Publishing Pool on the NAS server.

An Event Publishing Pool defines the CEPA servers and the specific events that trigger notifications.

After configuring the NAS server, you can enable events publishing on the file system from which you want to receive events. When a host generates an event on the file system over SMB or NFS, the information is forwarded to the CEPA server over an HTTP connection. The CEE CEPA software on the server receives the event and publishes it, thus enabling the third-party software to process it.

To use the Events Publishing Agent, it is required to have a PowerStore system with at least one NAS server configured on the network.

For additional information about CEPA, which is part of the Common Event Enabler (CEE), see *Using the Common Event Enabler on Windows Platforms* on the Dell Technologies Support site.

Create a publishing pool

To create an event publishing pool, you must have an Events Publishing (CEPA) server FQDN.

An Event Publishing Pool defines the CEPA server and the specific events that trigger notifications. Define at least one of the following event options:

- Pre Events - Events that are sent to the CEPA server for approval before processing.
- Post Events - Events that are sent to the CEPA server after they occur for logging or auditing purposes.
- Post Error Events - Error events that are sent to the CEPA server after they occur for logging or auditing purposes.

1. Select **Storage** > **NAS Servers**.
2. Select **NAS Settings**.
3. In the **Event Publishing** window, select **Publishing Pools** and then select **Create**.
4. Enter a **Pool Name**.
5. Enter the CEPA server FQDN.
6. In the Event Configuration section, click the event types and select the events that you want to add to the pool.
7. Click **Apply** to create the Events Publishing Pool.

Create an event publisher

After configuring publishing pools, create an event publisher to set the response to the different event types.

NOTE: Event publishers are created at the system level and one event publisher can be associated with multiple NAS servers.

1. Select **Storage** > **NAS Servers**.
2. Select **NAS Settings**.
3. Select **Event Publishers** and then select **Create**.
4. Continue to work through the **Create Event Publisher** wizard.

Wizard Screen	Description
Select Publishing Pools	• Enter a name. • Select up to 3 Publishing Pools. To create a new Publishing Pool, click **Create**.

Configure Event Publisher	• Pre-Events Failure Policy - Select the wanted behavior when all CEPA servers are offline for pre-events:
	  ○ Ignore (default) - Assume that all events are acknowledged.
	  ○ Deny - Deny events that require approval until CEPA servers are online.
	• Post-Events Failure Policy - Select the wanted behavior when all CEPA servers are offline for post-events:
	  ○ Ignore (default) - Continue operating. Events that occurred while the CEPA servers are down, will be lost.
	  ○ Accumulate - Continue operating and save events to a local buffer (up to 500 MB).
	  ○ Guarantee - Continue operating and save events to a local buffer (up to 500 MB). Deny access when buffer is full.
	  ○ Deny - Deny access to file systems when the CEPA servers are offline.
	• HTTP/Microsoft RPC
	• HTTP Port

5. Select **Apply** to create the Event Publisher.

Enabling an event publisher for a NAS server

After configuring the event publisher, enable it for the NAS server and all the file systems that are defined on it.

1. Select **Storage** > **NAS Servers** > **[nas server]**.
2. On the **Security & Events** page, select **Events Publishing**.
3. Select an Event Publisher from the list and enable it.
4. Select whether to enable the event publisher for all the file systems that are defined on the NAS server.

   Alternatively, you can select to enable the event publisher for specific file systems. For details, see Enable event publisher for file system.
5. Click **Apply**.

Enable event publisher for a file system

You can enable the event publisher for selected file systems.

1. Select **Storage** > **File Systems** > **[file system]**.
2. On the **Protection** page, select **Events Publishing**.
3. Enable the event publisher for the file system and select the protocol.
4. Click **Apply**.